

Navigating Compliance in eCommerce:

A Roadmap for Online Retail Success in the Healthcare Industry

PRESENTED BY:

Cassi Price | VGM Forbin

Kelly Grahovac | The van Halem Group



We Value and Request Your Feedback

With your help and input we can continue to deliver educational content that is the best in the industry! Feedback can be collected in 2 ways:

- 1. Please complete your session evaluation, handed out upon entry of this presentation, and return to the room monitor as you exit.**
- 2. You also have the option to complete your survey form in the mobile app. To complete through the app, go to conference agenda – locate & select the appropriate session - tap on the  to begin.**

Your feedback is greatly appreciated and helps provide us with first-hand insight that is carefully reviewed as we plan future Medtrade Conferences!

**DOWNLOAD THE
MEDTRADE SHOW
APP TO COMPLETE
SURVEY FORM**





Introducing



CASSI PRICE

President | VGM Forbin



KELLY GRAHOVAC

General Manager | The van Halem Group



Agenda

1

Why
eCommerce
in Healthcare

2

Security
First

3

Compliance
Next

4

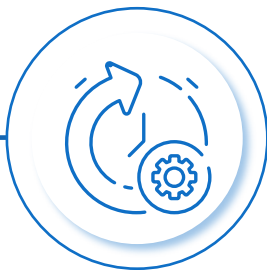
Competitive
Edge



Why eCommerce in Healthcare



Access to
Broader Audience



After-Hours
Service



New Revenue
Stream



Meeting the
Growing Demand
for Online Shopping
Options



Security FIRST

Without security, none of the business matters

1

PHI



2

SOC



3

SECURE
PAYMENT
GATEWAYS



PHI

THE RULE:

In eCommerce

- MFA
- Limited user access
- Strong encryption standards
- Firewalls
- Vulnerability scans

SOC

PAYMENT
GATEWAYS





PHI

SOC

PAYMENT
GATEWAYS

THE RULE: Compliance to ensure providers manage customer data securely

In eCommerce

- Trusted service principles for security availability, processing integrity, confidentiality, privacy.



PHI

SOC

Taking secure payment through:

- End-to-end encryption
- Fraud detection and prevention
- Multiple payment options
- Competitive transaction fees with no hidden charges

PAYMENT
GATEWAYS

authorize.net
A Visa Solution

 **Square**

TOP BRANDS

stripe

 **PayPal**

 **Rainforest**

 **worldpay**



MEDICARE



HIPAA



STATE LICENSURE



DATA PRIVACY



WCAG



TAX COMPLIANCE



MAP

Compliance NEXT

Why we're all here



Medicare

The Rules –

- Provider enrollment
- Data security and privacy
- Accurate billing and coding
- Compliance program
- Patient rights and communication
- Website policies
- Regular audits and updates



Medicare

In eCommerce

- Provider enrollment
 - Clearly state on your website that you are Medicare Licensed
- Data security and privacy
 - Protect patient information in
 - Form submissions
 - Marketing
 - Online Orders
 - Secure transactions
 - Encryption
 - Limited admins
- Accurate billing and coding
 - Detailed reporting and notes
- Compliance program
- Patient rights and communication
 - Pages dedicated to patient rights, policies and procedures
- Website policies
 - Pages dedicated to terms and conditions, privacy policies, refund/exchange policies, how to handle returns
- Regular audits and updates
 - Documentation of secure scans to protect against cyber threats and data breaches
 - Review updates to compliance laws



Advance Beneficiary Notice of Noncoverage (ABN) form

Inform Medicare beneficiaries that Medicare may not cover a specific item or they are choosing not to have Medicare cover a specific item.

This allows healthcare providers to prove Medicare beneficiaries are informed about potential out-of-pocket costs and can make informed decisions about their care.

Example of ABN in HMECommerce



HIPAA

In eCommerce

- **Data Encryption** – ensure ALL PHI is encrypted in transit and at rest
 - SSL
 - Emails
- **Secure Hosting** – ensure your hosting provider hosts in secure servers and data centers
- **Access Controls** – how many users are admins on your site? Do you have role-based access for admins that only need access to specific areas of your site?
- **Audits and Monitoring** – what is monitoring to detect security incidents?
- **Business Associate Agreements** – ensure all of your vendors who handle PHI have signed a BAA committing them to comply with HIPAA regulations
- **Incident Response Plan** – create and maintain an incident response plan for potential data breaches or security incidents

HIPAA

In Digital Marketing

- Retargeting
- Email Marketing





State Licensure

In eCommerce *(Regulations can vary by state)*

- State Tax Compliance
 - Automate applicable taxes by state, local, federal
 - Determine if state tax, VAT, or other taxes apply to your product/services
 - Automatically update rates and update on changes in tax regulations
- Data Privacy Laws also vary by state and country
- ADA – enforcement can vary by state





Data Privacy Laws

What is it:

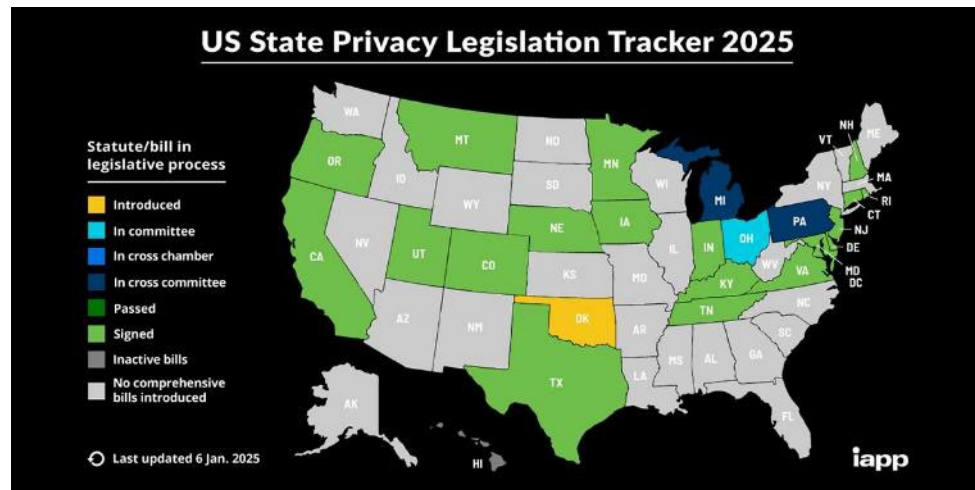
- **Personal Data Protection** – name, email address
- **Individual Rights** – right to access, correct, delete or be forgotten from your forms/emails, right to opt-out
- **Data Security** – appropriate security measures, breach notification requirements
- **Consent and Transparency** – must obtain consent or check boxes before collecting name and email, and must be transparent in policies on what data is collected and how it is used including cookies



Data Privacy Laws

Where is it:

- CCPA – California
- PIPEA – Canada
- GDPR – European Union
- LGPD - Brazil





WCAG or ADA

What is it:

- **Perceivable** – text alternatives to non-text content like images and videos through alt text and captions. Enable use of screen readers. Ensure appropriate color contrast and adjustable text.
- **Operable** – everything is accessible by keyboard, no time limits, there is clear headings and accessible forms.
- **Understandable** – clear language and defined abbreviations, consistent navigation and link labels, and input assistance on forms.
- **Robust** – compatible with current and future tools like assistive technology, proper HTML tags, etc.





WCAG or ADA

Where is it:

Not a law itself, but is widely adopted in regulatory framework for:

- **USA** – Americans with Disabilities Act and Section 508
- **European Union** – European Accessibility Act and EN 301 549
- **Canada** – Accessible Canada Act and Provincial Laws like Ontarians with Disabilities Act
- **Australia** – Disability Discrimination Act
- **United Kingdom** – Equality Act 2010





Compliance Automation Tool Recommendations:



AVALARA
Tax Compliance



**Secure
Privacy**

SECUREPRIVACY.AI
Data Privacy Compliance



ACCESSIBLE
ADA & WCAG Compliance





MAP or Minimum Advertised Price

A policy set by manufacturers to dictate the lowest price a product can be advertised by retailers

- **Brand Protection** – ensures products are not devalued
- **Retailer Support** – stable pricing environment, fair competition, avoids excessive discounting
- **Compliance and Enforcement** – violators will receive penalties, terminate business relationships, or reduce supply

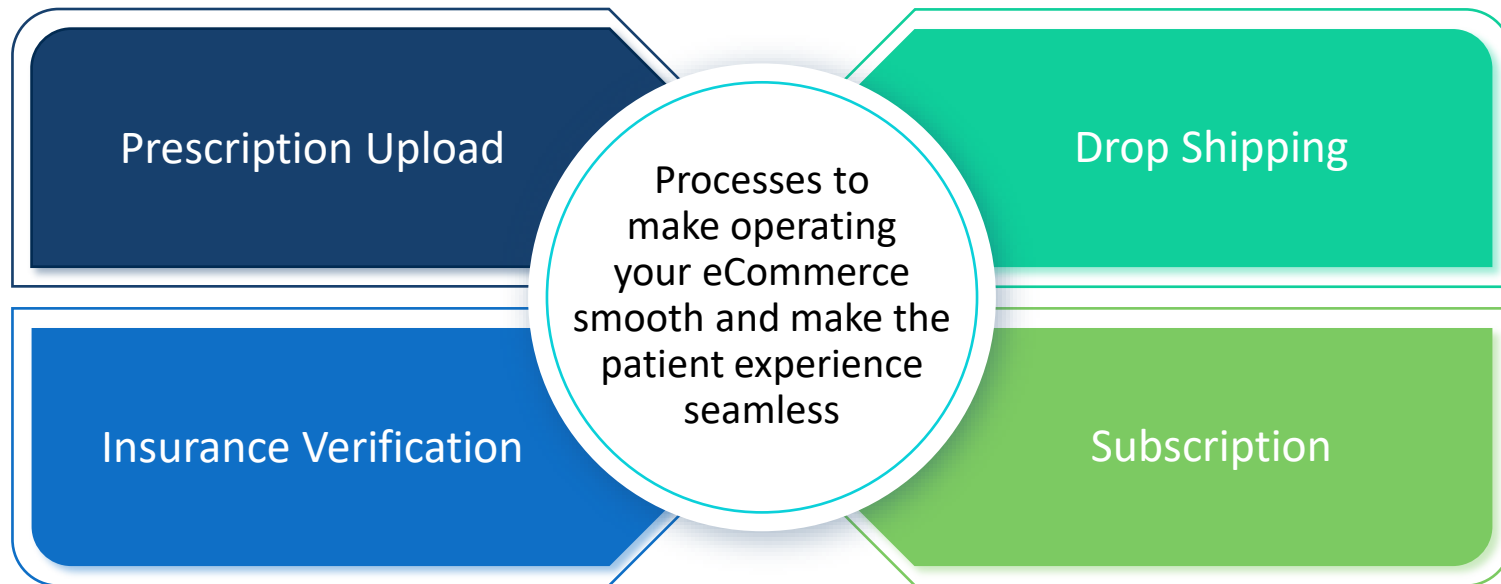
In eCommerce

- Look for a developer who understands MAP and has a connection to manufacturers to help you stay complaint



Competitive Edge

What will give you a competitive advantage on your eCommerce?





Prescription Upload Considerations

- **Compliance with Regulations** – ensure that the prescription upload process complies with HIPAA and other relevant regulations to protect patient information
- **Secure Data Handling** – use encryption for data in transit and at rest to safeguard sensitive information
- **User Authentication** – implement multi-factor authentication (MFA) to verify the identity of users uploading prescriptions
- **Ease of Use** – Design a user-friendly interface that simplifies the prescription upload process for patients and healthcare providers
- **Verification Process**– Establish a system for verifying the authenticity of uploaded prescriptions to prevent fraud



Insurance Verification Considerations

- **Automated Verification** - Utilize automated tools to verify insurance information quickly and accurately
- **Data Privacy** - Ensure that all insurance data is handled in compliance with data privacy laws such as HIPAA
- **Integration with EHR Systems** - Integrate the insurance verification process with electronic health record (EHR) systems for seamless data flow
- **Real-Time Updates** - Provide real-time updates on insurance verification status to both patients and healthcare providers
- **Clear Communication** - Clearly communicate any issues or discrepancies in insurance information to patients promptly



Drop Ship/Fulfillment Considerations

- **Reliable Partners** - Choose reliable drop shipping and fulfillment partners to ensure timely and accurate delivery of products
- **Inventory Management** - Implement robust inventory management systems to track stock levels and avoid stockouts
- **Order Tracking** - Provide customers with real-time order tracking to enhance their shopping experience
- **Compliance with Regulations** - Ensure that all fulfillment processes comply with relevant regulations, including state licensure and tax compliance
- **Customer Service** - Maintain excellent customer service to handle any issues that arise during the fulfillment process



Subscription Considerations

- **Flexible Plans** - Offer flexible subscription plans that cater to different customer needs and preferences
- **Automated Billing** - Implement automated billing systems to manage recurring payments efficiently
- **Customer Retention** - Use data analytics to understand customer behavior and improve retention rates
- **Compliance with Regulations** - Ensure that subscription services comply with relevant regulations, including data privacy and tax compliance
- **Value-Added Services** - Provide value-added services such as personalized recommendations and exclusive discounts to enhance the subscription experience



Key Takeaways

IMPORTANCE OF COMPLIANCE IN ECOMMERCE:

Protect patient information and maintain trust by complying with HIPAA, Medicare, and state licensure

Conduct regular audits, handle data securely, and communicate policies clearly



SECURITY MEASURES:

Implement encryption, MFA, and secure payment gateways to protect sensitive data

Comply with security standards like SOC 3 and PHI



COMPETITIVE EDGE THROUGH COMPLIANCE:

Use compliance automation tools to streamline operations and enhance customer trust

Tools like Avalara, SecurePrivacy.AI, and AccessiBe can help ensure regulatory adherence



QUESTIONS?

THANK YOU!

CASSI PRICE

President | VGM Forbin

cprice@forbin.com

(319) 874-6928

VGM**FORBIN**
— DIGITAL & IT



KELLY GRAHOVAC

General Manager | The van Halem Group

kelly@vanhalemgroup.com

(470) 225-7052

 The
van Halem
Group
A Division of VGM Group, Inc.





Schedule of Events

EXPO HALL HOURS

Wednesday, February 19 | 9:00AM – 5:00PM

Thursday, February 20 | 10:00AM – 3:00PM

Consultants Cocktail Hour

Tuesday, February 18 | 5:00PM – 6:15PM

AAHomecare Update

Wednesday, February 19 | 2:15PM – 3:15PM

**DOWNLOAD THE OFFICIAL MEDTRADE
2025 SHOW APP FOR A FULL SCHEDULE**

